A Practical Approach

Cyber Security and Technology

Cybersecurity with Cybers A Practical Approach

Code: 259009

FUTURE CENTRE
مركز المستقبل
futurecentre.net

Course Introduction

In today's interconnected world, cybersecurity is not just a technical concern but a business imperative. **Cybersecurity with Cybers: A Practical Approach** is designed to bridge the gap between theoretical knowledge and real-world application. This hands-on course leverages the **Cybers** framework—a structured, actionable methodology for implementing and managing cybersecurity defenses. Participants will learn to identify vulnerabilities, respond to incidents, and build resilient systems through immersive labs, simulations, and scenario-based exercises. Whether you're defending against ransomware or securing cloud infrastructure, this training provides the practical skills to protect organizations effectively.

Training Method

- Pre-assessment
- Live group instruction
- Use of real-world examples, case studies and exercises
- Interactive participation and discussion
- Power point presentation, LCD and flip chart
- Group activities and tests
- Each participant receives a binder containing a copy of the presentation
- slides and handouts
- Post-assessment

Course Objectives

Upon completion of this course, participants will be able to:

1. **Apply the Cybers framework** to assess and improve organizational security posture.
2. **Identify and mitigate common vulnerabilities** in networks, systems, and applications.
3. **Implement defensive measures** using tools like firewalls, IDS/IPS, and endpoint protection.
4. **Respond to security incidents** with structured containment and eradication strategies.
5. **Develop and enforce cybersecurity policies** aligned with industry best practices.
6. **Use automation and scripting** to streamline security operations.

Who Should Attend?

This course is ideal for:

- **IT professionals** seeking hands-on cybersecurity skills.
- **System and network administrators** responsible for security.
- **Security analysts** and **SOC team members**.
- **DevOps engineers** integrating security into workflows.
- **Compliance and risk management officers**.
- **Students and career-changers** entering the cybersecurity field.

Course Outline

Day 1: Foundations of Cybersecurity with Cybers

- **Module 1:** Introduction to the Cybers Framework: Principles and Workflow
- **Module 2:** Threat Landscape Overview: Attack Vectors, Threat Actors, and Motivations
- **Module 3:** Vulnerability Assessment and Risk Management
- **Hands-On Lab:** Setting Up a Lab Environment and Conducting a Basic Risk Assessment
- **Case Study:** Analyzing a Real-World Breach Using the Cybers Approach

Day 2: Network and System Defense

- **Module 4:** Secure Network Architecture: Segmentation, VLANs, and NAC
- **Module 5:** Implementing Firewalls, IDS/IPS, and VPNs
- **Module 6:** Endpoint Security: Antivirus, EDR, and Hardening Techniques
- **Hands-On Lab:** Configuring Firewall Rules and Deploying Endpoint Protection
- **Workshop:** Simulated Attack and Defense Exercise

Day 3: Application and Cloud Security

- **Module 7:** Securing Web Applications: OWASP Top 10 and Mitigation Strategies
- **Module 8:** Cloud Security Best Practices for AWS and Azure
- **Module 9:** DevSecOps: Integrating Security into CI/CD Pipelines
- **Hands-On Lab:** Identifying and Patching Vulnerabilities in a Web App
- **Group Exercise:** Securing a Cloud Deployment

Course Outline

Day 4: Incident Response and Automation

- **Module 10:** Incident Response with Cybers: Detection, Analysis, and Containment
- **Module 11:** Digital Forensics: Evidence Collection and Analysis
- **Module 12:** Automation with Scripting: Python and PowerShell for Security Tasks
- **Hands-On Lab:** Responding to a Ransomware Attack and Automating Remediation
- **Simulation:** Full Incident Response Drill

Day 5: Policy, Compliance, and Capstone Project

- **Module 13:** Cybersecurity Policies and Governance: NIST, ISO 27001, and GDPR
- **Module 14:** Security Awareness and Training for Employees
- **Module 15:** Developing a Cybersecurity Roadmap with Cybers
- **Capstone Project:** Designing and Implementing a Security Solution for a Fictional Organization
- **Course Wrap-Up:** Certifications, Career Guidance, and Q&A

المقدمة

في عالمنا المترابط اليوم، لم يعد الأمن السيبراني مجرد مسألة تقنية، بل أصبح ضرورةً عملية. صُممت دورة **"الأمن السيبراني مع خبراء الأمن السيبراني: نهج عملي" لسد الفجوة بين المعرفة النظرية والتطبيق العملي. تعتمد هذه الدورة العملية على إطار عمل خبراء الأمن السيبراني** ، وهو منهجية منظمة وقابلة للتنفيذ لتطبيق وإدارة دفاعات الأمن السيبراني. سيتعلم المشاركون كيفية تحديد نقاط الضعف، والاستجابة للحوادث، وبناء أنظمة مرنة من خلال مختبرات تفاعلية، ومحاكاة، وتمارين مبنية على سيناريوهات واقعية. سواء كنتم تدافعون ضد برامج الفدية أو تؤمّنون البنية التحتية السحابية، فإن هذا التدريب يوفر المهارات العملية اللازمة لحماية المؤسسات بفعالية.

طريقة التدريب

- التقييم المسبق
- تدريب جماعي مباشر
- استخدام أمثلة واقعية ودراسات حالة وتمارين
- مشاركة ونقاش تفاعلي
- عرض تقديمي باستخدام باور بوينت، وشاشة LCD، ولوح ورقي
- أنشطة واختبارات جماعية
- يحصل كل مشارك على ملف يحتوي على نسخة من العرض التقديمي
- شرائح ومطبوعات
- التقييم اللاحق

أهداف الدورة

عند الانتهاء من هذه الدورة، سيكون المشاركون قادرين على:

1. **تطبيق إطار عمل الأمن السيبراني** لتقييم وتحسين وضع الأمن التنظيمي.
2. تحديد نقاط الضعف الشائعة في الشبكات والأنظمة والتطبيقات **والتخفيف منها** .
3. **تنفيذ التدابير الدفاعية** باستخدام أدوات مثل جدران الحماية، وأنظمة الكشف عن التسلل/منع التسلل، وحماية نقاط النهاية.
4. **الاستجابة للحوادث الأمنية** باستخدام استراتيجيات احتواء واستئصال منظمة.
5. **تطوير وتنفيذ سياسات الأمن السيبراني** بما يتماشى مع أفضل الممارسات في الصناعة.
6. **استخدم الأتمتة والبرمجة النصية** لتبسيط عمليات الأمان.

من ينبغي أن يهتم؟

هذه الدورة مثالية ل:

- **متخصصون في تكنولوجيا المعلومات** يبحثون عن مهارات عملية في مجال الأمن السيبراني.
- **مسئولي النظام والشبكة** المسؤولين عن الأمن.
- **محللون أمنيون** وأعضاء **فريق مركز العمليات الأمنية** .
- **مهندسو DevOps** يقومون بدمج الأمان في سير العمل.
- **مسئولي الامتثال وإدارة المخاطر** .
- **الطلاب والراغبون في تغيير مسارهم المهني** والدخول في مجال الأمن السيبراني

محتويات الكورس

اليوم الأول أساسيات الأمن السيبراني مع خبراء الأمن السيبراني

- **الوحدة 1:** مقدمة إلى إطار الأمن السيبراني: المبادئ وسير العمل
- **الوحدة 2:** نظرة عامة على مشهد التهديد: متجهات الهجوم، والجهات الفاعلة في التهديد، والدوافع
- **الوحدة 3:** تقييم نقاط الضعف وإدارة المخاطر
- **مختبر عملي:** إعداد بيئة مختبرية وإجراء تقييم أساسي للمخاطر
- **دراسة حالة:** تحليل خرق حقيقي باستخدام نهج الأمن السيبراني

اليوم الثاني حماية الشبكة والنظام

- **الوحدة 4:** بنية الشبكة الآمنة: التجزئة، وشبكات VLAN، وNACg
- **الوحدة 5:** تنفيذ جدران الحماية، وأنظمة كشف التسلل/منع التطفل، وشبكات VPN
- **الوحدة 6:** أمان نقطة النهاية: مكافحة الفيروسات، والاستجابة للطوارئ، وتقنيات الحماية
- **مختبر عملي:** تكوين قواعد جدار الحماية ونشر حماية نقطة النهاية
- **ورشة عمل:** تمرين محاكاة الهجوم والدفاع

اليوم الثالث أمان التطبيقات والسحابة

- **الوحدة 7:** تأمين تطبيقات الويب: أفضل 10 استراتيجيات OWASP للتخفيف من المخاطر
- **الوحدة 8:** أفضل ممارسات أمان السحابة لـ AWS وAzureg
- **الوحدة 9:** DevSecOps: دمج الأمان في خطوط أنابيب CI/CD
- **مختبر عملي:** تحديد الثغرات الأمنية في تطبيق الويب وتصحيحها
- **تمرين جماعي:** تأمين نشر السحابة

محتويات الكورس

اليوم الرابع الاستجابة للحوادث والأتمتة

- **الوحدة 10:** الاستجابة للحوادث السيبرانية: الكشف والتحليل والاحتواء
- **الوحدة 11:** الأدلة الجنائية الرقمية: جمع الأدلة وتحليلها
- **الوحدة 12:** الأتمتة باستخدام البرمجة النصية: PowerShell و Python لمهام الأمان
- **مختبر عملي:** الاستجابة لهجوم برامج الفدية وأتمتة عملية الإصلاح
- **محاكاة:** تمرين الاستجابة الكاملة للحوادث

اليوم الخامس السياسة والامتثال ومشروع التخرج

- **الوحدة 13:** سياسات الأمن السيبراني والحوكمة: المعهد الوطني للمعايير والتكنولوجيا (NIST)، ومعيار ISO 27001، واللائحة العامة لحماية البيانات (GDPR)
- **الوحدة 14:** التوعية الأمنية والتدريب للموظفين
- **الوحدة 15:** تطوير خارطة طريق للأمن السيبراني مع خبراء الأمن السيبراني
- **مشروع التخرج:** تصميم وتنفيذ حل أمني لمنظمة خيالية
- **ملخص الدورة:** الشهادات والتوجيه المهني والأسئلة والأجوبة

Terms & Conditions

Complete & Mail to future centre or email

Info@futurecentre.com

Cancellation and Refund Policy

Delegates have 14 days from the date of booking to cancel and receive a full refund or transfer to another date free of charge. If less than 14 days' notice is given, then we will be unable to refund or cancel the booking unless on medical grounds. For more details about the Cancellation and Refund policy, please visit
https://futurecentre.net/

Registration & Payment

Please complete the registration form on the course page & return it to us indicating your preferred mode of payment. For further information, please get in touch with us

Course Materials

The course material, prepared by the future centre, will be digital and delivered to candidates by email

Certificates

Accredited Certificate of Completion will be issued to those who attend & successfully complete the programme.

Travel and Transport

We are committed to picking up and dropping off the participants from the airport to the hotel and back.

Registration & Payment

Complete & Mail to future centre or email

Info@futurecentre.com

Registration Form

- Full Name (Mr / Ms / Dr / Eng) .....
- Position .....
- Telephone / Mobile .....
- Personal E-Mail .....
- Official E-Mail .....
- Company Name .....
- Address .....
- City / Country .....

Payment Options

- ☐ Please invoice me
- ☐ Please invoice my company

Course Calander:

- 02/03/2026 - 06/03/2026 Click Now
- 20/07/2026 - 24/07/2026 Click Now
- 07/12/2026 - 11/12/2026 Click Now

VENUES

- LONDON
- BARCELONA
- KUALA LUMPER
- AMSTERDAM
- DAMASCUS
- ISTANBUL
- SINGAPORE
- PARIS
- DUBAI

OUR PARTNERS

THANK YOU

CONTACT US

+963 112226969

+963 953865520

Info@futurecentre.com

Damascus - Victoria - behind Royal Semiramis hotel

FUTURE CENTRE
مركز المستقبل

futurecentre.net